TITLE:

Grobner Basis の基礎(数式処理と数学研究への応用)

AUTHOR(S):

横山, 和弘

CITATION:

横山, 和弘. Grobner Basis の基礎(数式処理と数学研究への応用). 数理解析研究所講究録 1990, 722: 64-75

ISSUE DATE:

1990-05

URL:

http://hdl.handle.net/2433/101845

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
第 722 巻 1990 年 64-75

Gröbner Basis の基礎

富士通国際研 横山 和弘 (Kazuhiro YOKOYAMA)

近年の計算機の目覚ましい進歩に伴い数式処理システムが身近なものとなり、数式処理への関心も高まっている。さらに、計算機の高速化や記憶の大容量化により数式処理では難しいとされていた高度な代数操作が可能になってきた。中でも、一番の注目を浴びているのが、多項式イデアル論（計算機環論）と Gröbner 基底である。ここでは、この多項式イデアル論と Gröbner 基底に関する基礎的知識とその応用の話題を提供する。

1. はじめに

理工学のいろいろな分野では、解くべき対象の設定として、連立代数方程式を用い、その方程式の零点の集合として環境を設定している場合がある。この場合に問題となるのは、『情報を多項式に置き換る場合にどのように表現すべきか』である。すなわち、いくつかの多項式を連立代数方程式の束縛条件の下で扱う場合には、一見異なる多項式も実は同一のものであることがあったり、複雑な形をしていても、もっと簡単な形に書き換えることが可能であったりするのである。言い換えれば、ひとたび問題が連立代数方程式の束縛条件の下での多項式の性質へと置き換えられた時に、単純化 (simplification) や項書換え (term rewriting) の問題が発生するのである。この問題に明快な答を与えるのが、Gröbner 基底の理論である。そこで、簡単に Gröbner 基底とは何かを説明するならば、連立代数方程式に付随する多項式イデアルのイデアルとしての『いい性質を持った基底』であり、Gröbner 基底のいい性質とは、Gröbner 基底には付属する決定的な簡約操作 (M-reduction) が存在して、任意の多項式の連立代数方程式の束縛条件の下での一意表現がその簡約操作により計算できることである。Gröbner 基底を求める方法は、1960 年代に Buchberger により発見され、いくつかの改良を加えられて今日に至っている。現在では、この方法を Buchberger アルゴリズムと呼んでいる。

近年、英文での数式処理関連の本があいついで出版されており、それらにはアルゴリズム関係の話題も多く、当然 Gröbner 基底に関する解説記事も多い。残念ながら、日本語で書かれたもので、Gröbner 基底を解説している本はまだ出版されていない。日本語での解説として、古川氏等による大変分かり易く丁寧に書かれたものがいくつかあるが、その普及は今一歩であったようである。（この点が、日本における Gröbner 理論とその応用に関する研究者の少なさに

大きな影響を及ぼしているとも考えられる。）それらを読んでもらうのが一番よい方法であるが、書かれた時期が5～6年も前で、その後の進展等もあることなので、敢えて、古川氏等の筆致には遠く及ばないとは思いながらも、ここに解説を試みることにする。（最近では、神戸大の高山信毅氏による Gröbner 基底の解説があるので、興味のある方は高山氏に問い合わせて下さい。（残念ながら、当方では未入手。））以下、Gröbner 基底の定義と M- 簡約から紹介していく。

2. 多項式イデアルと Gröbner 基底

簡単に説明するために、対象を限定しよう。以下、多項式といえば変数が $x_1, ..., x_n$ であり、係数は有理数のものとする。有理数は0次の多項式とみなし、0は $-\infty$ 次の多項式とみなすことにする。この時、多項式全体のなす集合は環をなし、この環のことを、多項式環という。（$\mathbb{Q}[x_1, ..., x_n]$ で表す。）

多項式は、その名の通り、いくつかの項(term)の和の形で表される。項は、変数の積の部分(power product)とそれに係る有理数（係数）の二つの部分からなっている。

束縛条件（連立代数方程式）と簡約の問題

さて、多項式 g が多項式による束縛条件 $S = \{f_1 = 0, ..., f_r = 0\}$ の下でどのように表されるかを考えてみよう。1変数の場合であるならば、$g(x)$ は束縛条件 $f(x) = 0$ の下では、$g(x) = f(x)h(x) + r(x)$ なるユークリッド除算と、$f(x)h(x) = 0$ であることから次数が f より真に小さい多項式 r と同一視される。

これが多変数の場合でも g を $f_1, ..., f_r$ を使ってより小さい次数のものへと帰着できるかというとそうはうまくいかない。当然、二つの多項式 g_1, g_2 が束縛条件の下で、同じかどうかの判定も一筋縄ではいかない。ここで、『g_1, g_2 が束縛条件の下で同じである』とは、1変数の場合の拡張として考えれば、次の形になる。

『ある多項式 $a_1, ..., a_r$ が存在して、$g_1 - g_2 = a_1 f_1 + ... + a_r f_r$ である。』

（$f_1 = 0, ..., f_r = 0$ であるから、上の定義より、束縛条件の下では $g_1 = g_2$ になることがわかる。）

では、$f_1, ..., f_r$ にどのような性質があれば、上の問題が比較的楽に解けるかを考えてみよう。1変数の場合にユークリッド除算が有効であったのは、操作を一回するごとに次数が低く

なっていくことにある。すなわち、g を f で割った余りを取るという簡約操作において、『操作後の状態を表すインデックス』が『操作前の状態を表すインデックス』より小さくなっているのである。そこで、多変数の場合にも、この性質を持つような『インデックス』と簡約操作を捜せばよいことになる。（ここで、簡約操作とは、g からある f_i の多項式倍を引く操作であるとする。）

この『インデックス』として、各項に順序を導入し、多項式の順序はその項の順序の内で最大のものと定義する方法が Gröbner 基底には使われている。

大雑把に Gröbner 基底とは

ある順序と先の $f_1, ..., f_r$ から定まる多項式 $G_1, ..., G_s$ が、次の性質を持っているとする。

(G-1) 多項式 g が $a_1 f_1 + ... + a_r f_r$ の形に書けるならば g は $a'_1 G_1 + ... + a'_s G_s$ の形にも書け、逆も成り立つ。ここで、$a_1, ..., a_r, a'_1, ..., a'_s$ は多項式。

(G-2) 多項式 g に対して、$G_1, ..., G_s$ の元を利用した簡約操作が存在して、一回の操作において、必ず順序が低くなる。

上の簡約操作が更に、

(G-3) ある所で（有限回目）必ず停止し、

(G-4) みかけ上異なっている任意の多項式 g_1, g_2 に対してそれらの最終的に簡約化された多項式が一致する

という条件を満たすならば、与えられた多項式に対してその多項式を最終的に簡約された多項式に置き換えることで、束縛条件下の多項式の取り扱い問題を解決できることになる。この (1) (2) (3) (4) の条件を満たすような『うまい順序』と『うまい簡約操作』と『うまい多項式集合』が、admissible ordering、M-簡約、Gröbner 基底なのである。では、以下にもっときちんとした定義を与えてみよう。

多項式イデアルと生成元（基底）

多項式環の部分集合 $\mathcal{A}$ が次の条件を満たすときに $\mathcal{A}$ を多項式イデアル（簡単のためイデアル）と呼ぶ。

(I-1) $\mathcal{A}$ の任意の二元 a, b に対して、それらの和 $a+b$ も $\mathcal{A}$ の元である。

(I-2) $\mathcal{A}$ の任意の元 a と多項式環の任意の元 b に対して、それらの積 ab は $\mathcal{A}$ の元である。

有限個の多項式 f_1,...,f_r に対して、それらが生成するイデアル（ ideal$(f_1,...,f_r)$ と書く）は f_1,...,f_r を含む最小のイデアルとして定義される。

具体的には、ideal$(f_1,...,f_r)$ は $\{a_1f_1+a_2f_2+...+a_rf_r \mid a_1$,...,$a_r$ は多項式 $\}$ と書ける。（これを、生成するイデアルの定義に使うこともある。）

逆に、イデアル $\mathcal{A}$ に対してその生成元の集合 $\{f_1,...,f_r\}$（すなわち $\mathcal{A}$ =ideal$(f_1,...,f_r)$）をイデアルの基底とも呼ぶ。(基本的な定理により、多項式環のすべてのイデアルは、ある有限個の多項式から生成されるイデアルであることが知られている。)

このイデアルの概念を用いれば、『g_1 と g_2 が束縛条件の下で同一である』ということは、『g_1-g_2 が束縛条件に現れる多項式から生成されるイデアルに属する』ということに置き換えられる。また、大雑把な Gröbner 基底の節で示した、多項式の集合 $\{G_1,...,G_s\}$ は、イデアルの別の基底のひとつである。

うまい順序と簡約

以下、イデアル ideal$(f_1,...,f_r)$ を $\mathcal{A}$ とおく。先に多項式 g の $f_1,...,f_r$ による簡約を『g からある f_i の多項式倍を引く』として定義しておいた。この簡約の定義と大雑把な Gröbner 基底の定義の (G-2),(G-3) からうまい順序 (admissible) は次のような性質を持つべきである。

(O-1) 項の順序は項の変数の積部分 (power product) に現れる指数の作るベクトルの順序である。すなわち、項が $kx_1^{e_1}\cdots x_n^{e_n}$ とした時の、指数のなすベクトル $(e_1,...,e_n)$ 全体 $(\mathbf{Z}_0^+)^n$（ここで $\mathbf{Z}_0^+$ は非負整数全体）上の順序が項の順序を定める。

(O-2) 順序（$\leq$）は全順序である。

(O-3)（g からある af_i を引いていくのであるから、）3 個の積部分 a,b,c に対して、$a\leq b$ ならば $ac\leq bc$ である。また、積部分 a と $b\neq 1$ に対して、$a\leq ab$ である。

これでは、何のことやらわからないので、具体的な例を挙げてみよう。うまい順序としてよく使われるものには、『辞書式順序』と『全次数順序』の二つがある。これらの順序は唯一決まるわけでなく、『変数の順序』に依存していくつか決まるのである。そこで、うまい順序はかなりの数が存在する。ここでは、辞書式順序のひとつを説明する。

項 $T=x_1^{e_1}x_2^{e_2}\cdots x_n^{e_n}$ と $T'=x_1^{e_1'}x_2^{e_2'}\cdots x_n^{e_n'}$ に対して、$T>T'$ である $\leftrightarrow$ ある i（$i=0,...,n$）が存在して $e_1=e_1'$,...,$e_i=e_i'$ かつ $e_{i+1}>e_{i+1}'$ となる。

この順序は変数順序 $x_1>x_2>...>x_n$ による辞書式順序である。

さて、うまい簡約(M-簡約)は次になる。

(R-1) 多項式 g の多項式 f に関しての一回の M-簡約とは、

g のある項 T で、T が f の最大順序の項 H_f (頭項)の倍多項式である場合(すなわち、ある項 T' が存在して、$T = H_f T'$ となる場合)にのみ行う操作で、g から $T'f$ を引いて、項 T を消去することをいう。

(R-2) 多項式 g の多項式集合 $\{f_1, ..., f_r\}$ に関しての一回の M-簡約とは、

g のある項 T で、T がある f_i の最大順序の項 H_f (頭項)の倍多項式である場合にのみ行う操作で、多項式 g の多項式 f_i に関しての一回の M-簡約のことをいう。

g を多項式集合 $\{f_1, ..., f_r\}$ に関して何回も M-簡約して行くと、必ず有限回目でこれ以上 M-簡約できない所にまで行き着くことが簡単に示される。そこで、M-簡約をし尽くした最後の多項式($\underline{g}$ と書く)を『g の($\{f_1, ..., f_r\}$ に関して)簡約された多項式』(もしくは多項式集合が Gröbner 基底の場合には『g の正規形(normal form)』)と呼び、『g は $\underline{g}$ に($\{f_1, ..., f_r\}$ に関して)簡約される』という。

これで、やっと Gröbner 基底の定義ができる。

きちんと Gröbner 基底とは

うまい順序とその順序に対応する M-簡約があたえられている時に、イデアル $\mathcal{A}$ には、次の性質を持つ基底 $\Gamma = \{G_1, ..., G_s\}$ が存在する。この基底をイデアル $\mathcal{A}$ の Gröbner 基底と呼ぶ。

イデアル $\mathcal{A}$ のすべての元は、Γ に関して 0 に簡約される。

もちろん、Gröbner 基底の定義は他にいろいろとあり、どの定義が一番いいかとかは、Gröbner 基底を扱う人の問題意識によると思われる。まだきちんと述べていないものの内で結構大事だと思われることは、簡約された多項式へは、『簡約の順番に依らない』でたどり着くことである。M-簡約では、よく『どの項から消去しようか』という簡約の順番の問題が生じてしまう。Gröbner 基底でない多項式集合で M-簡約をした場合には順番を変えると全然違うものに行き着いてしまう場合が多々あるのである。この『簡約の順番に依らない』という性質は、決定的アルゴリズムにより、いつでも簡約された多項式が得られることを保証してくれているのである。

さて、実際の問題では、イデアルは、その生成元となるいくつかの多項式により与えられ

るものであるから、Gröbner 基底は、その生成元から何らかの方法で求めることになる。この方法として、Buchberger の方法がある。現在では、Buchberger の方法は、いろいろな数式処理システム上にインプリメントされており、ここでは、そのアルゴリズムには立ち寄らないことにする。というのは、今回の解説の主眼は、Gröbner 基底の性質とその応用にあるからである。(critical pair とか Church-Rosser 性と言った Buchberger の方法の理論的な面に興味のある方は、本解説文末の参考文献を参照されたい。) そこで、以下では、我々はすでに Gröbner 基底を計算する方法とこの基底に関する簡約方法を知っているものとする。以上、いままで述べた分をまとめてみると、次の図式ができる。

問題 $\Longrightarrow$ 連立代数方程式 $\{f_1 = 0, ..., f_r = 0\} \longrightarrow$ Gröbner 基底 Γ

$\longrightarrow \Gamma$ に関する M- 簡約 $\longrightarrow$ 束縛条件の下での簡約化 $\Longrightarrow$ 答

3. Gröbner 基底はよい基底

Gröbner 基底の持つ役に立つ性質とその応用について、『御本尊』の Buchberger が解説論文 (1985,1987) で詳しく述べている。ここでは彼の解説論文を大いに参考にして、Gröbner 基底のよい性質とその応用面を述べることにする。

最初に、若干の捕捉をしておく。Gröbner 基底は、先の定義のままでは与えられたイデアルに対して唯一定まるものではない。しかも、M- 簡約する時に、あまり必要がない元まで入っている場合もある。そこで、もう少し強い条件を加えることにより、より小さくて (唯一定まる) 基底が定義できる。これが、簡約された Gröbner 基底である。

簡約された Gröbner 基底

Gröbner 基底 Γ が簡約された Gröbner 基底であるとは、

Γ の任意の元 G に対して、G は $\Gamma \setminus \{G\}$ に関しては M- 簡約されない。

すべてのイデアルには、簡約された Gröbner 基底が存在し、しかも、それは係数倍を除いて唯一定まる。そこで、基底の各元の順序の最大の項の係数を 1 であるように取ることにすれば、唯一定まるものとなる。これを正規 Gröbner 基底と呼ぶ時もあるし、簡約された Gröbner 基底の定義に入れておく場合もある。ここでは、一応分けておく。(Buchberger の方法で求まるものは、これらの簡約された (正規) Gröbner 基底である。)

Gröbner 基底のよい性質

Buchberger(1987) は Theorem 2.5.1 (General Properties of Gröbner Bases) で、Gröbner 基底の基本性質を網羅している。ここでは、その抜萃を示す。以下では、$\mathcal{F}, \mathcal{G}$ は多項式の集合を表し、GB($\mathcal{F}$) はイデアル ideal($\mathcal{F}$) の正規 Gröbner 基底を表すものとする。また、NF(GB($\mathcal{F}$), f) で多項式 f の正規 Gröbner 基底 GB($\mathcal{F}$) に関する M- 簡約された多項式（正規形）を表すものとする。

(1) イデアルの合同性

二つのイデアルが同じものである ⇔ 正規 Gröbner 基底が一致する。

(ideal($\mathcal{F}$) =ideal($\mathcal{G}$) ⇔ GB($\mathcal{F}$) =GB($\mathcal{G}$))

(2) Gröbner 基底による簡約

二つの多項式がイデアル ideal($\mathcal{F}$) で合同 ⇔ イデアルの Gröbner 基底に関して M- 簡約された多項式が一致する。

($f \equiv g$ mod ideal($\mathcal{F}$) ⇔ NF(GB($\mathcal{F}$), f) =NF(GB($\mathcal{F}$), g))

(3) イデアルのメンバーシップ

多項式がイデアルに属する ⇔ イデアルの Gröbner 基底に関して M- 簡約された多項式が 0 である。

($f \in$ideal($\mathcal{F}$) ⇔ NF(GB($\mathcal{F}$), f) $= 0$)

(4) 剰余環での計算

多項式環をイデアルで割った剰余環は、正規形を元として定義される代数構造に同形である。すなわち、

$\mathbb{Q}[x_1, ..., x_n]$/ideal($\mathcal{F}$) なる剰余環は、元の集合として、$\{\text{NF}(\text{GB}(\mathcal{F}, f) \mid f \in \mathbb{Q}[x_1, ..., x_n]\}$ であり、その加法・乗法として次により定義されるものに同形となる。

$f \bigoplus g$ =NF(GB($\mathcal{F}$), $f + g$), $f \bigotimes g$ =NF(GB($\mathcal{F}$), fg)

(5) 剰余環を線形空間とみる

多項式環をイデアルで割った剰余環は線形空間である。その線形空間の基底としてイデアルの Gröbner 基底に対して M- 簡約できない単項式（係数が 1 である項）全体がとれる。すなわち、$\mathbb{Q}[x_1, ..., x_n]$/ideal($\mathcal{F}$) の基底として $\{u|$ u は Gröbner 基底 GB($\mathcal{F}$) の各元の順序が一番高い項（頭項）で割れない単項式 $\}$ が取れる。

(6) 自明なイデアル

イデアルが自明である（多項式環全体に一致する）⇔ Gröbner 基底に 1 がある。

(7) 連立代数方程式の解の個数の有限性

連立代数方程式の解は有限個である ⇔ 生成されるイデアルの Gröbner 基底の中に各 x_i のべきを最大順序の項（頭項）に持つ元がある。

以上は Gröbner 基底の定義より直接に導かれるものであった。次にチョットひねると導かれる性質を紹介する。

(8) 最小多項式

例えば『x_1 のみを変数とする多項式がイデアルの元としてあるかないか』という問題を考えてみよう。もしあるとするならば、この x_1 のみの 1 変数多項式の内で、次数最小の多項式の根はイデアルの零点の x_1 の値を示していることになる。このように、イデアルの次数最小の 1 変数多項式元は重要な意味を持つことがある。これを『最小多項式』と呼ぶことにする。まず、以下のことを線形代数の知識のみから導くことができる。

与えられた単項式の集合に対して、高々それらの項（係数倍を除く）のみからなる多項式がイデアルの元に存在する ⇔ 単項式の正規形の集合は、剰余環において線形従属である。

すなわち、$\{u_1, ..., u_r\}$ を単項式の集合とする時に、

$f \in \mathrm{ideal}(\mathcal{F})$ such that $f = \sum_{i=1}^{i=r} a_i u_i$ が存在する ⇔ $\{\mathrm{NF}(\mathrm{GB}(\mathcal{F}), u_i) \mid i = 1, ..., r\}$ は剰余環 $\mathbb{Q}[x_1, ..., x_n]/\mathrm{ideal}(\mathcal{F})$ 上で線形従属。（この線形従属関係は $\sum_{i=1}^{i=r} a_i \mathrm{NF}(\mathrm{GB}(\mathcal{F}), u_i) = 0$ ）

これを、$\{1, x_1, x_1^2, ...\}$ に応用すれば、もし x_1 を唯一の変数とする多項式が存在すれば、ある整数 r があって、$\mathrm{NF}(\mathrm{GB}(\mathcal{F}), 1)$, $\mathrm{NF}(\mathrm{GB}(\mathcal{F}), x)$,...,$\mathrm{NF}(\mathrm{GB}(\mathcal{F}), x^r)$ が線形従属になり、その従属関係より x_1 のみの多項式が得られる。r が最小になる時に得られた多項式は係数倍を除いて唯一定まる。これが x_1 の最小多項式である。

(9) シジジー (Syzygies) と線形不定方程式

多項式 f_1,...,f_r に対して、線形不定方程式

(9-1) $f_1 g_1 + f_2 g_2 + \cdots + f_r g_r = 0$

の多項式解 $(g_1, ..., g_r)$ （シジジーと呼ばれる）は線形空間をなすことがわかる。この解空間の基底は、Gröbner 基底を計算することにより求めることができる。

イデアル ideal$(f_1,...,f_r)$ の正規 Gröbner 基底 GB$(\{f_1,...,f_r\})$ を $\{G_1,...,G_s\}$ とすれば、各 G_i は $f_1,...,f_r$ の多項式係数線形和で書けている。すなわち、$G_i = a_{1,i}f_1 + \cdots + a_{r,i}f_r$ ゆえに (9-1) の線形不定方程式は、Gröbner 基底に関する線形不定方程式の解に帰着される。

(9-2) $G_1g_1 + G_2g_2 + \cdots + G_sg_s = 0$

そこで、次を定義する。

多項式 H に対して、H の正規形を $\underline{H}$ とおく。この時、$H = \underline{H} + \sum_{i=1}^{i=s} h_iG_i$ と書き表すことができ、ベクトル $(h_1,...,h_s)$ を随伴多項式ベクトルとでも呼んでおく。

さて、異なる $i < j$ に対して $S_{i,j} = t_jG_i - t_iG_j$ とおく。（この多項式操作は重大な意味を持つもので、一般に S-多項式と呼ばれている。）ここで、t_i は G_i の最大の順序の項（頭項）とする。この $S_{i,j}$ に対して、その随伴多項式ベクトルを $(h_{i,j,1}, h_{i,j,2}, ..., h_{i,j,s})$ とおく。この時に、(9-2) の解空間の基底として次が取れる。

$$\{(h_{i,j,1},..,h_{i,j,i-1}, h_{i,j,i} - t_i, h_{i,j,i+1}, ..., h_{i,j,j-1}, h_{i,j,j} + t_j, h_{i,j,j+1}, ..., h_{i,j,s})\}_{1\le i<j\le s}$$

これより、(9-1) の右辺が 0 でなく、多項式 H であった場合には、H の随伴多項式ベクトルを取ることにより、特殊解が求まる。これと先の解（一般解となる）を合わせて不定方程式の解を得る。

(10) 連立代数方程式の代数的解法

数学屋さんが結構好きな話題で、多くの研究がなされている。ここでは Buchberger が示した大変分かり易い基本的なものを示す。（残念ながら、この方法は実用的ではない。）今までは順序はなんでもよかったが、ここでは辞書式順序であると指定する。そして変数の順序は $x_n > x_{n-1} > ... > x_1$ とする。

さて、$\mathcal{F}$ を連立代数方程式に現れる多項式の集合とする。この時、次が成り立つ。

GB$(\mathcal{F})\cap\mathbb{Q}[x_1,...,x_i]$ はイデアル ideal$(\mathcal{F})\cap\mathbb{Q}[x_1,...,x_i]$ の Gröbner 基底となる。（これを i-th elimenation ideal と呼ぶ。）

これより、Gröbner 基底 GB$(\mathcal{F})$ の中には x_1 のみの多項式 $G_1(x_1)$, x_1 と x_2 の 2 変数多項式 $G_2(x_1,x_2)$,..., n 変数多項式 $G_n(x_1,...,x_n)$ が存在することがわかる。よって、G_1 の根 α_1 を求め、次に $G(x_1,x_2)$ の変数 x_1 に α_1 を代入し、$G_2(\alpha_1,x_2)$ の根 α_2 を求め,... といって、最後に $G_n(\alpha_1,...,\alpha_{n-1},x_n)$ の根 α_n を求めれば、連立代数方程式の解として、$(\alpha_1,...,\alpha_n)$ が求まる。

Gröbner 基底はもっと使える

基本性質を紹介してきたが、基本性質だけでもこんなにあるわけで、もっと工夫を加えれば、Gröbner 基底の利用法はいくらでも広がる。以下、思いつくままに書き出すと、数学的には、

多項式を成分とする行列の線形方程式の解法、

多項式間の代数的関係 (algebraic relation) を求める、

多項式写像の逆写像 (inverse mapping) を求める、

多項式の函数関係を求める (implicitization)、

イデアルの零点集合をパラメータで表す (parametrization)、

イデアルを準素分解 (primary decompostion) する、

イデアルの根基 (radical) を求める、

U- 終結式を求める、

代数方程式を効率よく解く、

D- 加群的方法による積分の計算、関数等式の定理証明

がある。

これらを利用した工学等の分野として、

ロボティックス、初等幾何の定理自動証明

が挙げられる。

4. Gröbner 基底はいいことばかりでないぞ

『きれいな花には刺がある』の喩え話のように、これだけよい性質を持つ Gröbner 基底には当然のごとく弱点がある。すなわち、計算量の問題である。辞書式順序での Gröbner 基底の計算は、いくら問題の大きさが小さくても、計算ステップの多さや、中間係数爆発等により現在の計算機では計算不能に陥ることが多い。Gröbner 基底の計算量の解析は、多くの研究者により調べられているが、実情を反映した結果はまだ得られていない。もとのイデアルが 0 次元である場合（結構小さい問題）でさえも、その計算量は生成する多項式の全次数の和に対して指数的であり、イデアルの次元について 2 重指数的であるという仮説もある。

さらに、順序の問題もある。一般に辞書式は効率が悪く、全次数順序の方が求まり易い。しかし、変数順序の選び方でも大きく計算量が変わってくるし、答となる Gröbner 基底の形

も変わってくる。この辺の問題が一番難しい所で、経験が一番ものを言うようでもある。（逆に、こうだから Gröbner 基底は面白いとも言える。）

では、だからと言って、『じゃあ使えないね』と見放なすのは早計である。これらの計算量の問題の克服のためにいくつかの研究がなされており、その克服も夢じゃないからである。例えば、現在の研究者は、直接的な計算の工夫としてモジュラ算法の導入を考えたり、間接的に、初めに比較的計算し易い順序で Gröbner 基底を求めておいて後でその基底を変換することで、自分の欲しかった順序での基底を求めることを考えたりしている。

その上、今後の計算機ハードの進歩により、このままでも Gröbner 基底の計算はかなりの問題でも解けるようになることが十分予想される。もし、その時に Gröbner 基底計算法をより効率よく求めるアルゴリズムを得ることができているならば、Gröbner 基底は幅広く応用されることになっているであろう。

5. さいごに

非常に大雑把に Gröbner 基底を紹介してきたが、さいごに Gröbner 基底の未来を考えて見よう。先にも述べたが計算機ハードの進歩は Gröbner 基底にとっては、願ってもない好条件である。しかし、この環境は Gröbner 基底だけに有利なわけではない。多項式イデアル論の立場から論ずれば、『ライバル』はいる。例えば、半世紀前の数学者 Ritt の研究をアルゴリズムに結び付けた呉教授の方法は、その解の部分性と計算の複雑さ等により Gröbner 基底ほど普及していない。しかし、呉教授の弟子等は地道にその改良を行っており、計算機の性能アップは呉教授派の方法にも好条件であるので、十分 Gröbner 基底派に対抗しうると思われる。さらに、現在の計算機による多項式イデアル論の研究はダイナミックに動きつつあり、理論面の研究は Gröbner 基底に代わる新しいものを生み出す可能性すらある。

とにかく、現在の『期待の星』 Gröbner 基底は近未来において実用になるのは確かなことである。

参考文献

残念ながら、Gröbner 基底のみを扱った書籍はなく、Gröbner 基底の記事はその一部の章に現れる。以下に参考文献の内で、主なもののみを列挙する。

Gröbner 基底の紹介・応用を扱ったものとして、Buchberger 自らが書いたものとして、

B. Buchberger(1985), Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory: Recent Trends in Multidimensional Systems Theory, Chap.6, D. Reidel Publ. Comp.

B. Buchberger(1987), Applications of Gröbner Bases in Non-Linear Computational Geometry: Trends in Computer Algebra, Lecture Notes in Computer Science, Springer-Verlag, p.52-80.

最近の本では、

J. H. Davenport, Y. Siret, E. Tournier(1988), Computer Algebra, Chap.3, Academic Press.

C. Hoffmann(1989), Geometric & Solid Modeling: An Introduction, Chap.7, Morgan Kaufman.

日本語の紹介・解説記事としては、

古川昭夫, 小林英恒 (1984), Gröbner-Basis とその応用, 数理科学講究録 520, p.23-35.

古川昭夫 (1985), Gröbner-Base について, 数式処理通信 Vol.3-No.1, サイエンティスト社, p.15-32.

佐々木建昭, 古川昭夫 (1986), コンピュータ環論, 情報処理, Vol.27-No.4, p.404-413.

Simplification 等の概念からみた立場のものとして、

B. Buchberger, R. Loos(1982), Algebraic Simplification: Computer Algbera Symbolic and Algebraic Computation, Springer-Verlag, p.11-44.

Geomtry Theorem Proving の立場からの最近の本として、

S. C. Chou(1988), Mechanical Geometry Theorem Proving, Reidel Publ..